PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-186667
(43)Date of publication of application : 16.07.1996

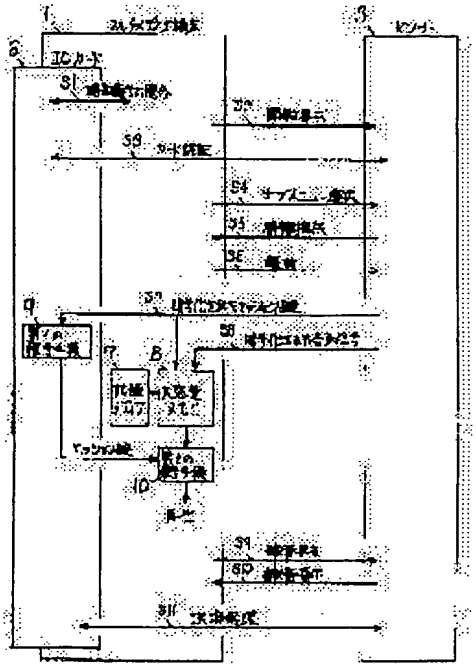
(51)Int.Cl. H04M 15/00
G06F 15/00
G09C 1/00
G10K 15/04
H04H 1/02
H04L 9/00
H04L 9/10
H04L 9/12
H04N 7/173

(21)Application number : 07-000257
(22)Date of filing : 05.01.1995

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : TAKAGI SHINYA

(54) DIGITAL INFORMATION RECORDING SYSTEM

(57)Abstract:
PURPOSE: To prevent legal digital copy from being performed by a user while protecting the right of a software author in a system of transmitting music software and video software to individuals through the use of a digital network.
CONSTITUTION: An IC card 6 is used as a control part and has a secret card key (k) peculiar to this card. On the other hand, by a request from a multi- media terminal 1, digital information ciphered by a session key (s) and the session key (s) ciphered by the card key (k) are sent from a center 3 to the multi-media terminal 1 and recorded in a recording media 7. At the time of reproducing digital information, digital information is restored by the session key (s) deciphered in the IC card 6.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平8－186667

(43)公開日　平成８年(1996)７月16日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｍ　15/00		Ｚ		
Ｇ０６Ｆ　15/00	３３０	Ｚ　9364－5L		
Ｇ０９Ｃ　1/00		7259－5Ｊ		
Ｇ１０Ｋ　15/04	３０２	Ｄ		
			Ｈ０４Ｌ　9/00	Ｚ

審査請求　未請求　請求項の数３　ＯＬ　（全９頁）　最終頁に続く

(21)出願番号　特願平7－257

(22)出願日　平成７年(1995)１月５日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　高木　伸哉
大阪府門真市大字門真1006番地　松下電器産業株式会社内

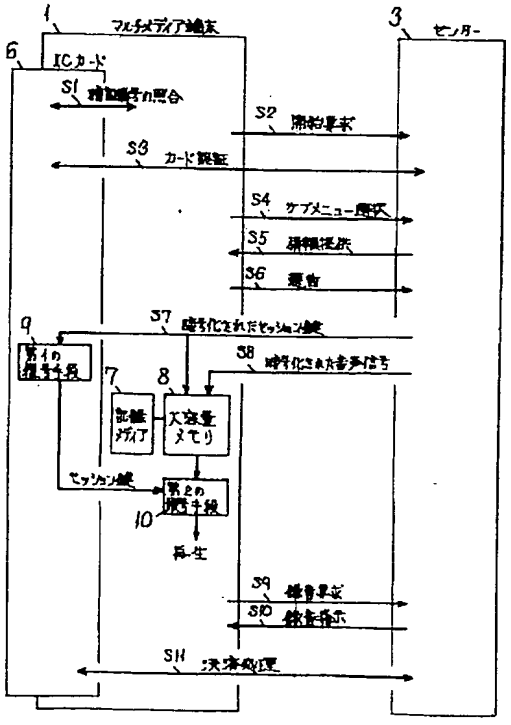
(74)代理人　弁理士　小鍛治　明　（外２名）

(54)【発明の名称】　デジタル情報記録システム

(57)【要約】

【目的】　デジタルネットワークを用いて音楽ソフトや映像ソフトを個人向けに伝送するシステムにおいて、ソフト著作者の権利を守りながらユーザによる正当なデジタルコピーが防止できるシステムを提供する。

【構成】　ＩＣカード６を制御部として、このカードに固有で秘密のカード鍵ｋをもたせる一方、マルチメディア端末１からの要求によりセンター３からマルチメディア端末１に、セッション鍵ｓで暗号化されたデジタル情報と、カード鍵ｋで暗号化されたセッション鍵ｓが送られ、記録メディア７に記録される。デジタル情報を再生する際には、ＩＣカード６内で復号されたセッション鍵ｓによりデジタル情報が復元される。



1

【特許請求の範囲】

【請求項１】デジタル情報のデータベースを保有する情報センターと、この情報センターに接続され前記センターへデジタル情報の送信を要求する要求手段と、デジタル情報を記録メディアへ書き込む書き込み手段とを有する端末を備え前記センターは端末使用者の正否を判断して正の場合に端末からの要求に応じてデジタル情報を端末へ送信する送信手段と、送信したデジタル情報の記録メディアへの書き込み手段を制御する制御手段とを有することを特徴とするデジタル情報記録システム。

【請求項２】デジタル情報のデータベースを保有する情報センターと、この情報センターに接続され前記センターへデジタル情報の送信を要求する要求手段と、デジタル情報を記録メディアへ書き込む書き込み手段とを有する端末と第１の鍵を格納する格納部を有するＩＣカードを備え、前記センターは端末使用者の正否を判断して正の場合に端末からの要求に応じてデジタル情報を端末へ送信する送信手段と、送信したデジタル情報の記録メディアへの書き込み手段を制御する制御手段とデジタル情報を暗号化する第２の鍵を発生する手段と、前記第１の鍵と前記第２の鍵から第３の鍵を演算する手段と、前記第２の鍵によってデジタル情報を暗号化する手段とを有し、前記ＩＣカードは前記第１の鍵と前記センターから送信される第３の鍵から第２の鍵を演算する手段を有し、端末は前記センターから送信される暗号化されたデジタル情報を前記ＩＣカードから送信される第２の鍵により、デジタル情報を復元する手段を有することを特徴とするデジタル情報記録システム。

【請求項３】ＩＣカードは、第４の鍵を発生する手段と第５の鍵を格納する格納部とを有し、センターの制御手段は、第４の鍵と第１の鍵から第５の鍵を演算し、端末の書き込み手段は、前記第５の鍵によって制御されることを特徴とする請求項２記載のデジタル情報記録システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、通信回線、例えば大容量のデジタルネットワークを用いて、音楽ソフトや映像ソフトを個人向けに伝送し、記録するシステムに関する。

【０００２】

【従来の技術】近年、通信技術およびコンピュータ技術の発達により、情報のデジタル化が進んでおり、新しい魅力的なサービスが生まれつつある。例えば、これまでの放送とは違い、ユーザが好きな時に見たい映像ソフトを情報センター（以後センターという）要求すると、センターからそのユーザに要求した映像ソフトが送られてくる、いわゆるビデオ・オン・デマンドという新しいシステムが実験的に進められており、注目されている。

【０００３】

2

【発明が解決しようとする課題】また同様のシステムで映像ソフトではなく、音楽ソフトに関するサービスへも展開が可能である。特に音楽ソフトの場合は映像ソフトと違い１曲あたりの時間が短く、繰り返し聴きたい場合も多い。その度にセンターにアクセスするのではユーザにとって料金が嵩んでしまい、またアクセスする手間が面倒であり、更にシステムにおいてトラヒックの問題が発生する。

【０００４】ユーザにとっては、１回聴くための料金は比較的低額で、気に入った曲は自分の端末にデジタル録音し、それ以降はセンターへアクセスすることなく繰り返し聴けることが望ましい。しかしながら、比較的低額な料金を支払っただけで個人の端末にデジタル録音可能というシステムでは著作権が保護されないという問題がある。

【０００５】また、このシステムにおいてユーザの本人確認が暗証番号の照合で行われているという問題がある。なぜなら暗証番号による、本人確認の安全性の低さは周知の通りであり、サービスが拡大するほど、またサービスが魅力的になるほど不正使用される可能性が大きく、本人確認の安全性を高める必要がある。

【０００６】また、このシステムは、システムを利用したユーザではなく、端末に対して課金されるため、ユーザはどの端末でも自由には使用できなかった。その点、ユーザ本人に課金されるシステムであれば、どの端末でも自由にこのシステムを利用できることとなり、利便性が増す。

【０００７】本発明は、上記の問題点を解決するものであり、著作者の権利を守り、かつ、ユーザによる映像、音楽ソフト等のデジタル記録が可能となるシステムを提供することを目的とするものである。

【０００８】また、ユーザの本人確認の安全性を高め、ユーザ本人に課金されるシステムを提供することを目的とするものである。

【０００９】

【課題を解決するための手段】本発明は上記目的を達成するために、端末に装備される記録メディアへのデジタル情報の書き込み手段は、端末使用者の正否を判断し、正の場合にセンターの制御手段により、制御される構成である。また、端末がＩＣカードを受け入れる装置を有し、ＩＣカードはそのカードに固有の秘密の鍵コード（以後カード鍵という）を有しており、録音されたデジタル情報は秘密データを用いて演算が施されており、ＩＣカードはカード鍵を用いて前記秘密データを復元する手段を有する構成としたものである。

【００１０】

【作用】上記構成により、デジタル情報はユーザの正否の照合の後、センターの制御によってのみ記録メディアへ記録可能であり、また記録されたデジタル情報はＩＣカードを用いてのみ再生可能となり、著作者の権利は保

護される。また、ＩＣカードは秘密のカード鍵を用いることによって、このシステムへのアクセスツールおよび決済ツールとしても使用できるものである。

【００１１】

【実施例】

（実施例１）以下、本発明の一実施例について図面を参照しながら説明する。図１は本発明の一実施例におけるシステムの概略を示す図であり、ユーザが所有するマルチメディア端末１はネットワークＩＳＤＮ２を通して、音楽ソフトを管理しているセンター３および銀行４と接続されている。センター３と銀行４間はこの場合伝送する情報量が多いため、例えば専用回線５で結ばれている。マルチメディア端末１は、ディスプレイ、スピーカの他、ＩＣカード６を挿入するためのリーダライタと、音声信号を録音するための記録メディア７用のドライバを有している。

【００１２】図１で示した本システムに用いるＩＣカード６の発行について説明を行う。ユーザがセンター３に対して本システムへの加入申請を行うと、センター３は銀行４にＩＣカード６の発行を依頼する。銀行４はＩＣカード６にユーザの暗証番号や個人情報等、本カードを銀行業務で使用するために必要な情報を書込み、センター３に渡す。センター３ではＩＣカード６に会員番号ｎ、カード鍵ｋを書き込んでユーザに渡す。ここで、カード鍵ｋは秘密の暗号鍵であり、次式により算出される。

【００１３】ｋ＝Ｆ（ｎ）

ここでＦはセンター３のみが知る秘密の関数であり、ｎは会員番号である。上記式により、カード鍵ｋは会員番号ｎの関数であり、それぞれのカードに固有（すなわちユーザに固有）である。ＩＣカード６にこれらを書き込んだ後は、会員番号ｎを読み出すことは可能であるが、カード鍵ｋは決して読み出すことができないものである。しかし、センター３はＩＣカード６から会員番号ｎを読み出すことにより、カード鍵ｋを再算出することができる。よって、会員番号ｎとカード鍵ｋをＩＣカード６に書き込んだ後は、これらの情報をセンター側で持っておく必要はない。

【００１４】ユーザはＩＣカード６を受け取った後、マルチメディア端末１（以下、単に端末１と記す）を用いて銀行４にアクセスし、自分の銀行口座の残高の中から希望金額をＩＣカード６内の口座へ移す。もちろん、この処理を行うためには暗証番号の照合が必要であるが、これらの手続きについてここでは詳細は省略する。

【００１５】次に、図２を用いて本実施例のシステムを利用する際の処理の流れを説明する。

【００１６】まず、ユーザがＩＣカード６を端末１に挿入すると、例えば端末１のディスプレイ上に０～９までの１０個の数字と、暗証番号の入力を促すメッセージが出力される。ここでユーザがディスプレイに表示された数字を指で押し、スイッチの投入で正しい暗証番号を入力することにより、ＩＣカードが暗証番号の照合を行い（ステップＳ１）、端末１は本システムの利用を開始するための開始要求をセンター３に送信する（ステップＳ２）。センター３はこの要求を受信することによりサービスを開始する。まず最初にセンター３によるＩＣカード６の認証が行われる（ステップＳ３）。これはＩＣカード６が正当なカードであるか否かを確認するためのものであり、正当なカードでない場合、サービスは打ち切られる。

【００１７】カード認証が正常に終了すると、ディスプレイ上にメインメニューが表示される。このメインメニューは端末１を使用して受けられるサービス等の一覧であり、ユーザはこの中から例えば「音楽鑑賞」を選択する。このメニューが選択されるとディスプレイ上には、ジャンル、アーチスト名、年代等、ユーザが曲を選択する際に手助けとなるサブメニューが表示される。ユーザは例えば聴きたい曲のアーチスト名が決まっている場合は具体的なアーチスト名を指定する。また、タイトルやアーチスト名が不明であったり、聴きたい曲が具体的に決まっていない場合、ディスプレイ上に「冬の情景を描いたフォークソング」といった選択枝を表示し指定させてもよい。このようにユーザがサブメニューから希望の選択枝を指定すると、その情報が端末１からセンター３へ送信される（ステップＳ４）。センター３は送られてきた情報をもとにデータベースを検索し、該当する全ての曲のタイトルを情報として端末１に提供する（ステップＳ５）。ユーザがディスプレイに表示されたタイトル一覧から聴きたい曲を指定すると、端末１はセンター３へ選曲情報を送信する（ステップＳ６）。

【００１８】曲が指定されると、センター３は音声信号を暗号化するための鍵をランダムに生成し（以後、この鍵をセッション鍵という）、これをカード鍵ｋで暗号化してＩＣカード６へ送信する（ステップＳ７）。これと同時に音声信号をセッション鍵で暗号化し、端末１へ送る。暗号化された音声信号は端末１の大容量メモリ８に一旦格納される（ステップＳ８）。一方暗号化されたセッション鍵はＩＣカード６の第１の復号手段９で復号され、元のセッション鍵に復元される。この復元されたセッション鍵を用いて第２の復号手段１０により、大容量メモリ８に格納されている暗号化された音声信号は元の音声信号に復元され、曲の再生が可能となる。その後端末１のディスプレイ上の「スタート」という表示を指で押すと、演奏が開始される。

【００１９】演奏が終わると、ディスプレイには例えば（１）鑑賞、（２）録音、（３）終了の選択枝が表示される。別の曲を聴きたい場合は（１）を選択し、ステップＳ６またはステップＳ４から同様の処理を繰り返す。また、今聴いた曲を録音したい場合は（２）を選択する。（２）が選択されると、その情報がセンター３へ送

られる（ステップＳ９）。センター３が録音指示を端末１に送ると（ステップＳ１０）、大容量メモリ８から記録メディア７へ暗号化された音声信号が書き込まれる。これにより、ＩＣカード６を所持する正当なユーザは、繰り返しその曲を聴くことができ、また、バックアップや編集のような個人利用のために暗号化された音声信号をデジタルコピーすることも可能である。しかし、記録メディア７の内容を別の記録メディアにコピーして複製を作ったとしても、書き込まれた音声信号は暗号化されているため、このユーザのＩＣカード６がないと音声信号を復元し再生することはできない。このようにして、不正コピーを防止することができる。

【００２０】本サービスを終了する場合は（３）を選択すると、決済処理へ移る（ステップＳ１１）。決済処理では、録音しなかった場合、聴いた回数分だけＩＣカード６の口座から料金が差し引かれるが、これは比較的低額に設定される。一方、録音を行った場合は、録音料金が差し引かれるが、これは比較的高額に設定される。

【００２１】次に各ステップを説明する。図３はステップＳ３のカード認証の一例を示したものである。まず、ＩＣカード６は会員番号格納部１１に格納されている会員番号ｎをセンター３へ送信する。センター３はカード鍵演算部１２において関数Ｆを用いて会員番号ｎからカード鍵ｋを算出する。カード鍵ｋは各ＩＣカードに固有の秘密番号である。すなわち、カード鍵ｋは、このＩＣカード６のみが有し、センター３のみが会員番号ｎから算出し得る秘密の番号であり、カード認証、コピー防止、決済というセキュリティに関する全ての処理に使用される極めて機密性の高いデータである。

【００２２】次にセンター３は乱数生成手段１３を用いて乱数ｒを生成し、ＩＣカード６へ送信する。ＩＣカード６は演算部１４により、カード鍵格納部１５に格納しているカード鍵ｋを用いて乱数ｒに演算Ｇを施し、センター３へ送信する。このデータをｘ１とすると、ｘ１は次式で表される。

【００２３】ｘ１＝Ｇ（ｋ，ｒ）

センター３は演算Ｇを行う演算部１６を有しており、先に算出したカード鍵ｋで乱数発生手段１３が生成した乱数ｒに演算Ｇを施し、ｘ２を算出する。比較手段１７はｘ１とｘ２を比較し、これらが等しい場合、ＩＣカード６がカード鍵ｋを有する正当なカードであるとみなし、カード認証のステップＳ３を正常に終了する。ｘ１とｘ２が異なっている場合は、不正なカードによるアクセスであるため、サービスは打ち切られる。

【００２４】次に図４を用いてセッション鍵の配送（図２のステップＳ７）および音声信号の送信（ステップＳ８）を説明する。まず、センター３はセッション鍵生成手段１８を用いてセッション鍵ｓをランダムに生成する。そして、暗号化手段１９において演算Ｇを施し、前述のカード鍵ｋによりセッション鍵ｓを暗号化してＩＣカード６に送信する。このデータをｙとすると、ｙは次式で表される。

【００２５】ｙ＝Ｅ（ｋ，ｓ）

ＩＣカード６は暗号化手段１９によってｙをセッション鍵ｓに復元する第１の復号手段９を有しており、これを用いてカード鍵ｋによりｙをセッション鍵ｓに復元する。

【００２６】次にセンター３は暗号化手段２１において関数Ｐを用いて音声信号ｍを上記セッション鍵ｓで暗号化し、端末１へ送信する。このデータをｚとすると、ｚは次式で表される。

【００２７】ｚ＝Ｐ（ｓ，ｍ）

このデータｚは大容量メモリ８に一旦格納された後、第２の復号手段１０において第１の復号手段９で復元されたセッション鍵ｓにより元の音声信号ｍに復元される。

【００２８】また、同じく図４を用いて録音要求（図２のステップＳ９）が出された場合の処理と再生方法について説明する。端末１の録音要求部２２からの録音要求を受けてセンター３の録音指示部２３により録音指示が出された場合、ドライバ２４を介して暗号化されたデータｙと暗号化されたデータｚが記録メディア７に記録される。録音されたデータｚを再生するとき、記録メディア７に記録された暗号化されたセッション鍵のデータｙがＩＣカード６に入力され、前述と同じ処理によりセッション鍵ｓが復元され、それを用いて暗号化されたデータｚから元の音声信号ｍが復元される。

【００２９】このようにカード鍵ｋを有するＩＣカード６を用いれば音声信号ｍの復元が可能となるが、ＩＣカード６がなければ、セッション鍵ｓを復元することができないため、音声信号ｍも復元することができない。

【００３０】（実施例２）次にＩＣカード６を所持するユーザが、ドライバ２４を何らかの理由により操作し、センターが録音指示を出していないにもかかわらず記録メディア７への録音処理が行なわれた場合、このユーザはＩＣカード６の所持者自身であるから音声信号の再生が可能である。すなわち、このユーザは録音のための料金を支払うことなく録音が可能となる。

【００３１】この操作を防止する方法を図５を用いて説明する。図５は録音要求が出された場合の処理方法に関する他の実施例を示したものである。ステップＳ７、Ｓ８については同様であるため、説明を省略する。ステップＳ９、Ｓ１０について説明するとＩＣカード６が鍵処理部２５とセッション鍵格納部２６を有しており、ユーザからの録音要求があった場合（ステップＳ９）、鍵処理部２５は乱数ｕを生成し、出力する。録音要求部２２はこの乱数ｕをセンター３へ送信する。録音指示部２３は、この乱数ｕをカード鍵ｋで暗号化してデータｖを生成し、ｖとともに録音指示を端末１に送信する（ステップＳ１０）。これにより、ドライバ２４を介して暗号化された音声信号データｚが記録メディア７に記録され

る。本実施例では、暗号化されたセッション鍵データｙは記録メディア７には記録されない。一方、信号データｖはＩＣカード６に与えられ、鍵処理部２５により検証される。この検証結果が正しければ、セッション鍵ｓ′がセッション鍵格納部２６に書き込まれる。再生の際には、この格納されたセッション鍵ｓ′が読み出され、音声信号ｍの復号のために使われる。本実施例では、ユーザが前記のような操作を試みても、ＩＣカード６は物理的に安全であるため、鍵処理部２５を操作してセッション鍵ｓ′を不正に書き込むことはできない。また、録音指示部２３からの信号データｖを偽造しようとしても、この信号データｖはカード鍵ｋと乱数をもとに暗号化されているため、偽造は不可能である。このように、録音指示により音声信号ｍを復号するためのセッション鍵ｓ′をＩＣカード６に書き込む方法を採用することにより、なお一層、セキュリティを向上させることができる。

【００３２】ただし、再生の際にＩＣカード６から読み出されるセッション鍵ｓ′の盗聴に関しては注意を払わなければならない。なぜならば、盗聴されたセッション鍵ｓ′を記録した媒体と、暗号化された音声信号の複製との組み合わせにより、音声信号の再生が可能となるからである。

【００３３】これを防ぐための一つの手段は、ＩＣカード６からセッション鍵ｓを読み出して音声信号全体を復号するのではなく、復号手段１０とＩＣカード６とが連動して音声信号ｍを復号することである。例えば、音声信号の復号の一部をＩＣカード６内で行うようにする。この復号処理をＩＣカード６に行わせるためのＩＣカード６への命令は、制御情報として、暗号化された音声信号がｍに付加して記録メディア７に記録される。このような処理を複雑にし、かつ秘密にすることにより、単なるセッション鍵ｓ′の盗聴で音声信号ｍを再生することは不可能となり、セキュリティはより一層向上する。

【００３４】最後に決済処理（図２のステップＳ１１）について図６を参照しながら説明する。センター３のトランザクションデータ送信部２７は会員番号、日付、金額等の情報からなるトランザクションデータｔをＩＣカード６に送信する。ここで金額については既に述べたとおり、録音しなかった場合と、録音した場合では、差が設けてある。ＩＣカード６の署名生成部２８は、ＩＣカード６内の口座の残高から支払額を減算した後、署名鍵格納部２９に格納された署名鍵ｃを用いて関数Ｈによりトランザクションデータｔに対する署名データａを生成する。署名データａは、

ａ＝Ｈ（ｃ，ｔ）

で表され、センター３に送信される。センター３はメモリ３０にトランザクションデータｔと署名データａとを対にして記録する。

【００３５】ここで署名鍵ｃはＩＣカード６に固有であり、図１の銀行４のみが知る秘密鍵である。センター３も署名鍵ｃを知らないので、署名データａを偽造することはできない。したがって、署名データａはトランザクションデータｔに対するユーザの署名とみなすことができる。これらのデータを図１の専用回線７を用いて銀行２に送信することにより、銀行２内で処理が行われ、決済が完了する。

【００３６】これまで述べてきた通り、ＩＣカードを用いた本実施例のシステムにより、ユーザは相応の料金を支払えば音楽ソフトをデジタル録音することが可能となる。その他、ＩＣカードを用いることにより、本実施例は次の効果を奏する。

【００３７】まず第１に、システムへのアクセスツールとしてＩＣカードを用いているため、ＩＣカードを所持し、かつ、そのＩＣカードの暗証番号を知らなければシステムにアクセスできないため、暗証番号のみによるアクセスに比べセキュリティが高い。

【００３８】第２に、決済処理がＩＣカードを用いて行われているため、ユーザはＩＣカードさえ所持しておれば、どの端末を用いても本サービスを受けることができるという点である。すなわち、ユーザはいろんな場所にいながらにして、このシステムを利用できることとなり、利便性が増す。

【００３９】本実施例では、音楽ソフトの場合を例に上げて示したが、これに限定されることなく、本発明は映像ソフト、ゲーム等、デジタル化された情報に関するあらゆるサービスに適用し得るものである。

【００４０】

【発明の効果】以上のように本発明によれば、ＩＣカードに格納された秘密のカード鍵によってのみ、記録メディアに記録されたデジタル情報が復元可能となるため、このＩＣカードがなければ実質的なコピーは得られなく不法コピーを防止できる。また、センターからの録音指示により、デジタル情報を復元するための秘密情報をＩＣカード内に書き込む手段を設けることにより、正当な支払をすることなくデジタル録音するようなユーザの操作を防止することができる。さらに、ＩＣカードのカード鍵を用いてカード認証を行うことにより、不正アクセスに対する防御を強固にできる。また、ＩＣカードのカード鍵を用いて決済処理を行うことにより、端末ではなくＩＣカードによる決済が可能となり、ユーザは本システムを利用するための端末を限定されることなく利便性が大きい。

【図面の簡単な説明】

【図１】本発明の一実施例におけるシステムの概略を示す図

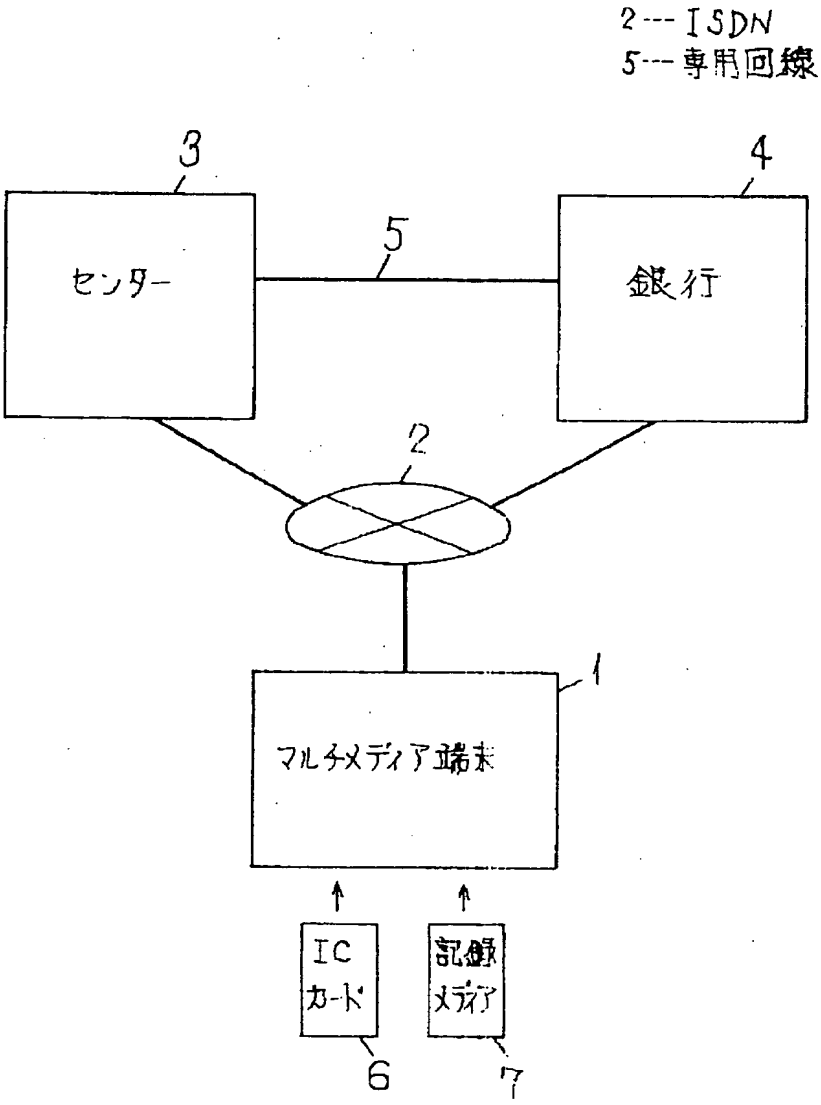
【図２】本発明の一実施例の処理フローを示す図

【図３】本発明の実施例のカード認証ステップのブロック図

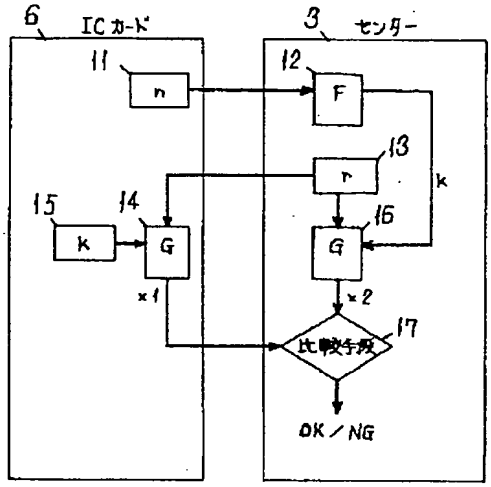
【図４】本発明の実施例のデジタル情報の送信および録

音ステップのブロック図
【図５】本発明の他の実施例のデジタル情報の送信および録音ステップのブロック図
【図６】本発明の実施例の決済ステップのブロック図
【符号の説明】
1　マルチメディア端末
2　ＩＳＤＮ
3　センター
4　銀行
5　専用回線
6　ＩＣカード
7　記録メディア

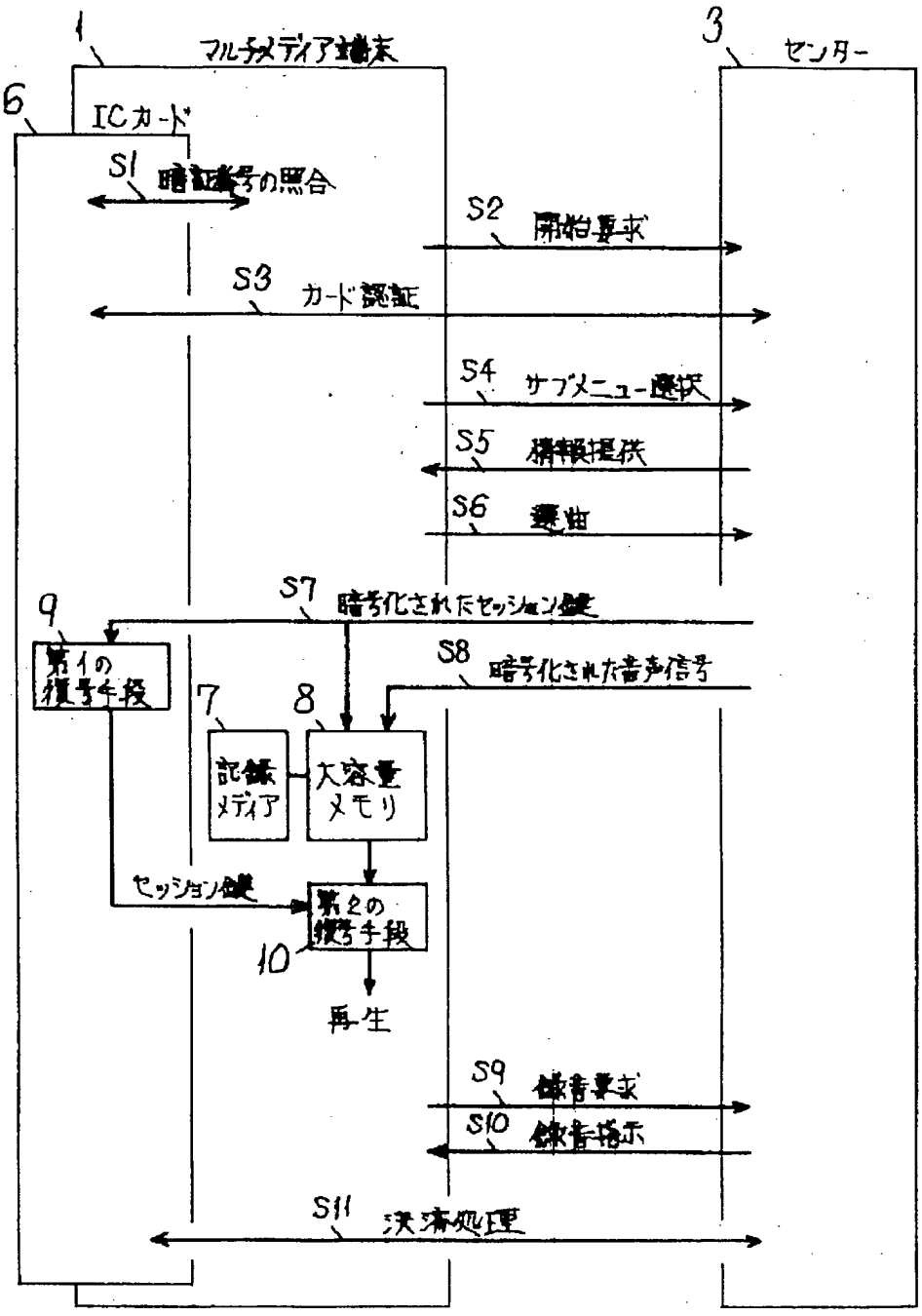
【図１】



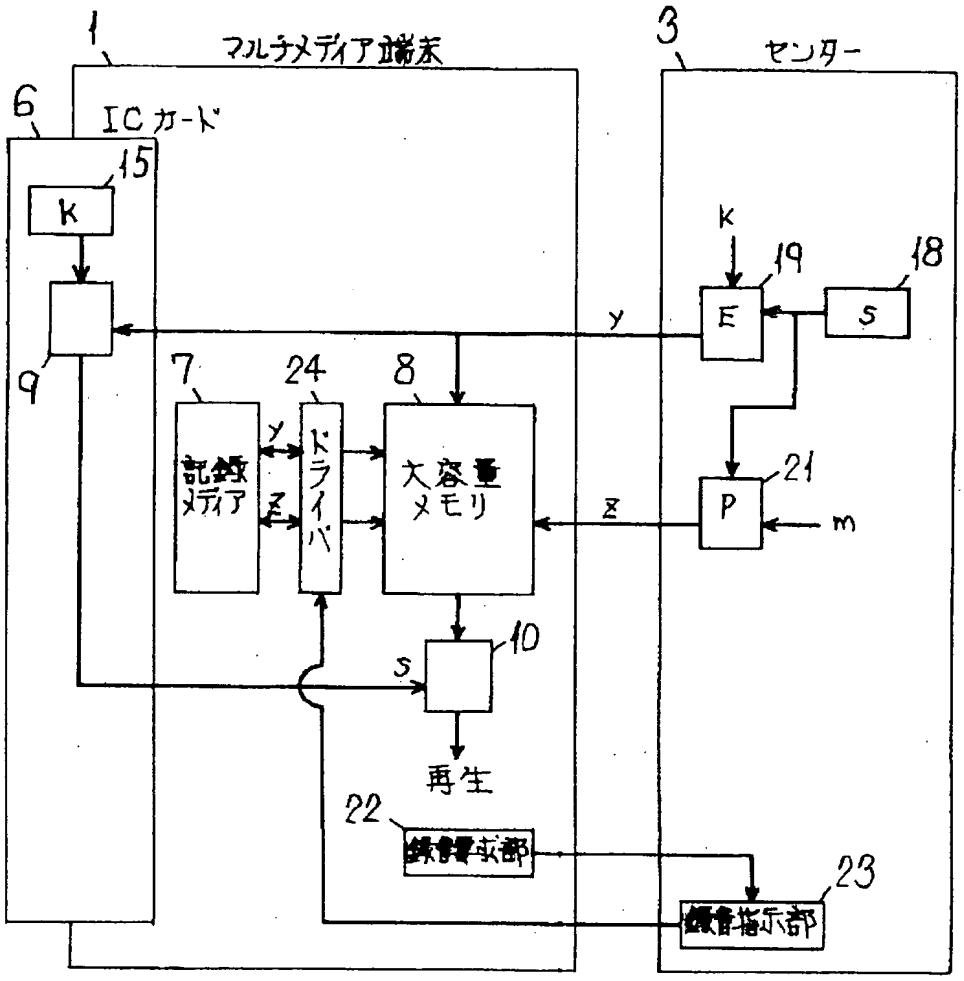
【図３】



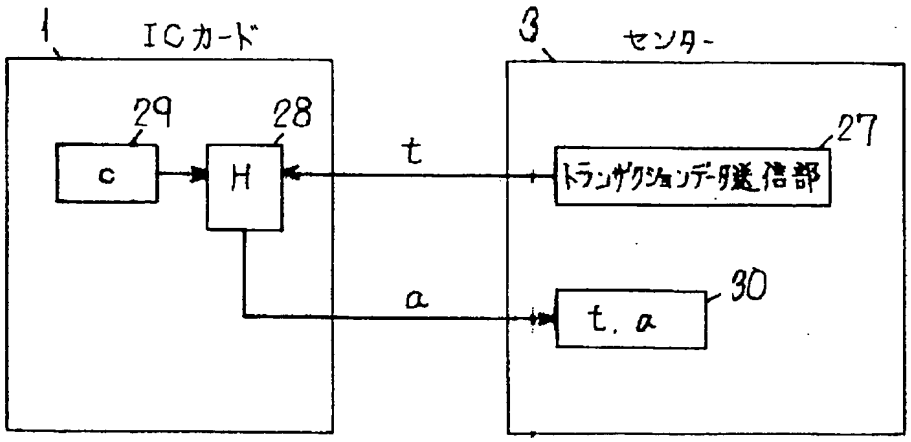
【図２】


1
マルチメディア端末
3
センター
6
ICカード
S1
暗証番号の照合
S2
開始要求
S3
カード認証
S4
サブメニュー選択
S5
情報提供
S6
選曲
S7
暗号化されたセッション鍵
9
第1の復号手段
S8
暗号化された音声信号
7
記録メディア
8
大容量メモリ
セッション鍵
第2の復号手段
10
再生
S9
録音要求
S10
録音指示
S11
決済処理

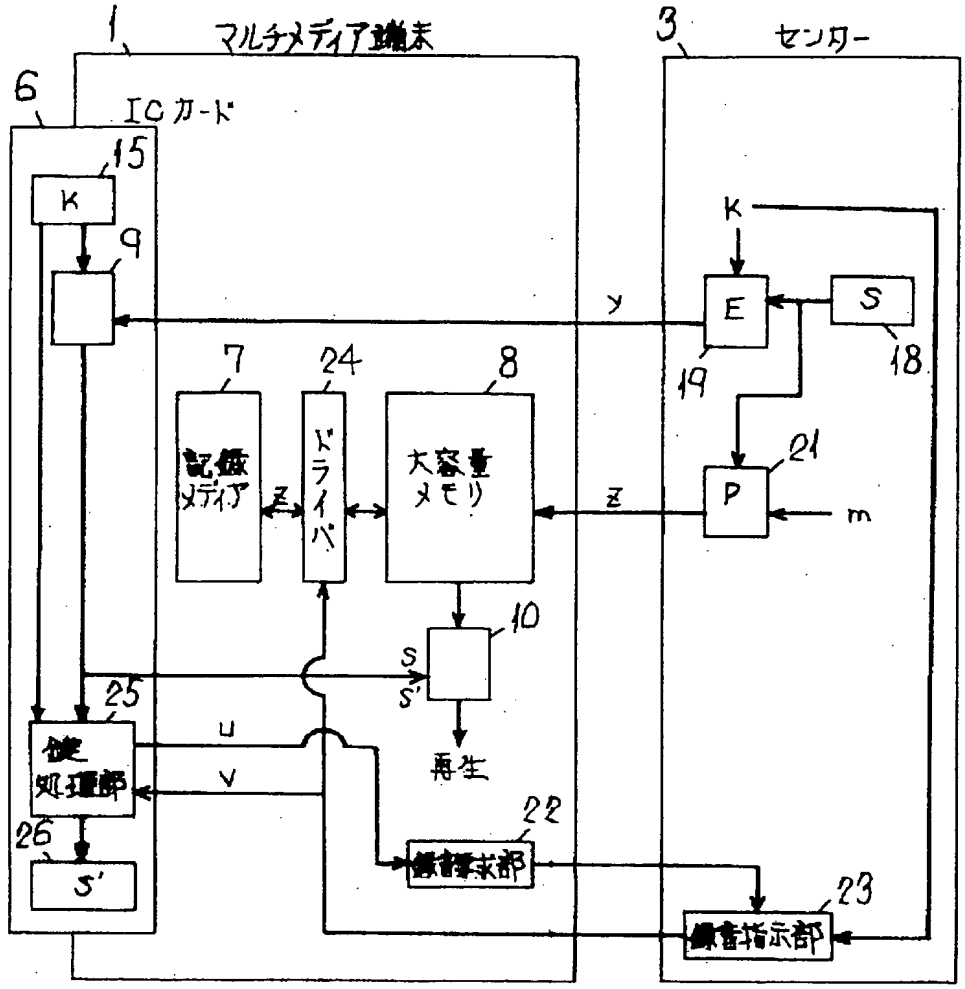
【図４】


1
マルチメディア端末
3
センター
6
ICカード
15
K
9
7
24
8
記録メディア
y
z
ドライバ
大容量メモリ
K
19
18
E
S
y
z
P
21
m
10
s
再生
22
23

【図６】


1
ICカード
3
センター
29
28
c
H
t
27
トランザクションデータ送信部
a
30
t, a

【図５】



フロントページの続き

(51) Int. Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｈ	1/02			Z	
				E	
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｈ０４Ｎ	7/173				